Encryption of Covert Information into Multiple Statistical Distributions

R. C. Venkatesan

Systems Research Corporation
I.T.I Rd., Aundh, Pune 411007, India
Email: ravi@systemsresearchcorp.com

Abstract

A novel strategy to encrypt covert information (code) via unitary projections into the *null spaces* of ill-conditioned eigenstructures of multiple host statistical distributions, inferred from incomplete constraints, is presented. The host *pdf*'s are inferred using the maximum entropy principle. The projection of the covert information is dependent upon the *pdf*'s of the host statistical distributions. The security of the encryption/decryption strategy is based on the extreme instability of the encoding process. A self-consistent procedure to derive keys for both *symmetric* and *asymmetric* cryptography is presented. The advantages of using a multiple *pdf* model to achieve encryption of covert information are briefly highlighted. Numerical simulations exemplify the efficacy of the model.

Key words: Statistical encryption/decryption, projections, ill-conditioned eigenstructures, inference, maximum entropy.
PACS: 05.20.-y, 02.50.Tt, 02.30.Zz, 07.05.Kf, 89.70.+c

1 Introduction

The success of prominent contemporary cryptosystems is attributed to the degree of difficulty in computing integer factorizations [1] and discrete logarithms [2, 3], respectively. This paper describes a novel strategy to encode covert information via unitary projections into the *null spaces* of the eigenstructures of a hierarchy of host statistical distributions (multiple *pdf*'s). The multiple *pdf*'s are inferred from an incomplete set of constraints (physical observable's) using the maximum entropy (MaxEnt) principle [4]. Here, a multiple *pdf* model is defined as a hierarchial ensemble of *pdf*'s $p^{\nu}; \nu = 1, ...$. The index ν is defined

as the *hierarchy index*. This paper defines the host *pdf*'s p^ν to deviate from the equilibrium state, with increasing values of ν.

The case of incomplete constraints corresponds to scenarios where the number of constraints (physical observable's) is less than the dimension of the distribution. In a discrete setting, the MaxEnt Lagrangian for a single host *pdf* $p^\nu(x_n) = p_n^\nu; n = 1, ..., N$ is [4]:

$$L^{ME} = -\sum_{n=1}^{N} p_n^\nu \ln p_n^\nu + \sum_{i=0}^{M}\sum_{n=1}^{N} \lambda_i^\nu p_n^\nu \Theta_i\left(x_n\right), \tag{1}$$

$M < N$, where the Lagrange multiplier (LM) λ_o^ν corresponds to the *pdf* normalization condition $\sum\limits_{n=1}^{N} p_n^\nu = 1$. The LM's $\lambda_i^\nu; i = 1, ..., M$ correspond to physical constraints of the form $\sum\limits_{n=1}^{N} p_n^\nu \Theta_i\left(x_n\right) = d_i^\nu; i = 1, ..., M$. Here, $\Theta_i\left(x_n\right); i = 1, ..., M$ is an operator, and, $d_i^\nu; i = 1, ..., M$ are the incomplete constraints. This paper employs geometric moment constraints, i.e. $\Theta_i\left(x_n\right) = x_n^i; i = 1, ..., M$. Solution of (1) yields:

$$\begin{array}{l} p_n^\nu = \exp\left[-\sum\limits_{i=0}^{M} \lambda_i^\nu x_n^i\right]; n = 1, ..., N, \\ and, \\ e^{\lambda_o^\nu} = \sum\limits_{n=1}^{N} e^{-\lambda_i^\nu x_n^i}; i = 1, ..., M. \end{array} \tag{2}$$

Solution of (2) for a given input set of LM's, is referred to as the *forward MaxEnt problem*. Inference of *pdf*'s and the concomitant LM's, given an input set of $d_i^\nu; i = 1, ..., M$, is referred to as the *inverse MaxEnt problem*.

Statistical distributions inferred from incomplete constraints possess eigenstructures that are ill-conditioned. These demonstrate extreme sensitivity to perturbations. This sensitivity is exploited to formulate a principled framework to encrypt/decrypt code [1]. The *null spaces* of these eigenstructures constitute an "invisible reservoir" into which covert information may be projected. The projection is achieved without altering the host statistical distributions. The advantage of statistical encryption is that the dimension of the code that can be encrypted increases with the size of the statistical distribution. The projection of code into a host statistical distribution is also a promising candidate to implement steganography [5], and, related disciplines in information hiding [6].

[1] In this paper, the terms *code* and *covert information* are used interchangeably.

A recent study has treated the statistical encryption/decryption of covert information, using the Fisher information as the measure of uncertainty [7]. Qualitative distinctions vis-á-vis an equivalent MaxEnt formulation [8] have been established. The encoding strategies in [7] and [8] are *independent* of the *pdf* of the host statistical distribution. Encoding covert information into multiple *pdf*'s allows code of dimension greater than that of any single host *pdf* to be selectively encrypted into the multiple *pdf*'s. An example of this is the encryption of multi-dimensional code defined in matrix form, such as image data. In this case, each dimension of the code (column/row vector of the matrix) may be selectively encoded into individual components (single host *pdf*'s) of a multiple host *pdf* model. Each single host *pdf* is taken to be one dimensional in the *continuum*.

Conversely, the dimension of each host in a multiple *pdf* model may be chosen by the designer to be less than the dimension of the code. This is tantamount to effecting a tradeoff between the dimension of a single host *pdf*, and, the number of hosts comprising a multiple *pdf* model. *The success of employing multiple pdf's to enhance the security of the covert information, is critically contingent upon the encryption/decryption strategy being dependent upon the pdf's of the statistical hosts.* This feature permits the *pdf* dependent statistical encryption/decryption strategy to possess immense qualitative flexibility, as compared with *pdf* independent models [7, 8]. Numerical simulations demonstrate impressive quantitative performance in securing covert information.

2 Projection of the Covert Information

Consider M constraints $d_1^\nu, ..., d_M^\nu$. In a discrete setting, these are expectation values of a random variable $x_{i,n}; n = 1, ..., N$:

$$d_i^\nu = \sum_{n=1}^{N} p_n^\nu x_{i,n}; i = 1, ..., M. \tag{3}$$

Evoking the Dirac *bra-ket* notation [9], the *pdf* $|p^\nu\rangle \in \Re^N$ which is a column vector (*ket*), where $|n\rangle ; n = 1, ..., N$ is the standard basis in $\Re^N$, is expressed as $|p^\nu\rangle = \sum_{n=1}^{N} |n\rangle \langle n \mid p^\nu\rangle = \sum_{n=1}^{N} p_n^\nu |n\rangle$. Defining the column vector of observable's as $|d^\nu\rangle \in \Re^{M+1}$ with components $d_1^\nu, ..., d_M^\nu, 1$, and, an operator $A : \Re^N \to \Re^{M+1}$ given by $A = \sum_{n=1}^{N} |x_n\rangle \langle n|$. Defining vectors $|x_n\rangle \in \Re^{M+1}; n = 1, ..., N$ as the expansion $|x_n\rangle = \sum_{i=1}^{M+1} |i\rangle \langle i \mid x_n\rangle = \sum_{i=1}^{M+1} x_{i,n} |i\rangle$,

where i is a basis vector in $\Re^{M+1}$, (3) may be expressed simply as:

$$|d^\nu\rangle = A\,|p^\nu\rangle\,; A : \Re^N \to \Re^{M+1}. \tag{4}$$

The physical significance of the constraint operator A in (4) is as follows. Inference of the *pdf* from physical observable's employing (2) is achieved by specifying $\Theta_i\left(x_n\right) = x_n^i$. Setting, $x_n^i \to x_{i,n}; i = 1, ..., M; n = 1, ..., N$, the $x_{i,n}$ constitute the elements of the M rows and N columns of the operator A^ν. The unity element in $|d^\nu\rangle \in \Re^{M+1}$ enforces the normalization of $|p^\nu\rangle$. Consequently, $x_{M+1,n} = x_n^{M+1} = 1; n = 1, ..., N$.

The operator A *is independent of the host pdf.* This qualitative deficiency may be rectified by defining:

$$\tilde{A}^\nu = A + k^\nu\,|d^\nu\rangle\,\langle I|\,. \tag{5}$$

Here, $\langle I|$ is a $1\times N$ row vector (*bra*), and, $k^\nu \neq -1$ is a constant parameter introduced to adjust the condition number of $\tilde{A}^\nu$, and hence its sensitivity to perturbations. In (5), dependence upon the host *pdf* is "injected" into the operator $\tilde{A}^\nu$ by the incorporation of $|d^\nu\rangle$. Specifically, each element of the *ket* $|d^\nu\rangle$ is defined by $d_i^\nu = \sum\limits_{n=1}^{N} p_n^\nu x_n^i; i = 1, ..., M$.

Re-defining (4) in terms of (5) yields: $\tilde{A}^\nu\,|p^\nu\rangle = |d^\nu\rangle + \langle k^\nu\,|d^\nu\rangle\,\langle I|\rangle_\nu$, where $\langle\bullet\rangle_\nu$ signifies the expectation evaluated at the *hierarchy index* ν . Expanding $\langle k^\nu\,|d^\nu\rangle\,\langle I|\rangle_\nu = k^\nu\,|d^\nu\rangle\,\langle I|\,p^\nu\rangle$, and evoking the *pdf* normalization: $\langle I|\,p^\nu\rangle = 1$, yields:

$$\left|\tilde{d}^\nu\right\rangle = (k^\nu + 1)\,|d^\nu\rangle = \tilde{A}^\nu\,|p^\nu\rangle\,; \tilde{A}^\nu : \Re^N \to \Re^{M+1}. \tag{6}$$

The operator $\tilde{A}^\nu$ is ill-conditioned and rectangular. Thus, (6) becomes:

$$|p^\nu\rangle = \left(\tilde{A}^\nu\right)^{-1}\left|\tilde{d}^\nu\right\rangle + \left|p^{\nu'}\right\rangle, \tag{7}$$

where, $\left(\tilde{A}^\nu\right)^{-1}$ is the pseudo-inverse [10] of $\tilde{A}^\nu$, and lies in $range\left(\tilde{A}^\nu\right)$. All necessary data dependent information resides in $\left(\tilde{A}^\nu\right)^{-1}\left|\tilde{d}^\nu\right\rangle$.

The *null space* term in (7) is of particular importance since the code is encoded into it via unitary projections. Here, $\left|p^{\nu'}\right\rangle \in null\left(\tilde{A}^\nu\right)$ is explicitly data independent [2] . However, it is critically dependent on the solution methodology

[2] In this paper, *null* () signifies the *null space* of an ill-conditioned operator, unless explicitly specified as being the $MATLAB^{®}$ routine to calculate the normalized

employed to solve (7). To define the unitary projections of the embedded code, the operator $G^{\nu} = \tilde{A}^{\nu\dagger}\tilde{A}^{\nu}$ is introduced. Here, $\tilde{A}^{\nu\dagger}$ is the conjugate transpose of $\tilde{A}^{\nu}$. For real matrices, $\tilde{A}^{\nu\dagger} = \tilde{A}^{\nu T}$, where $\tilde{A}^{\nu T}$ is the transpose of $\tilde{A}^{\nu}$.

It is legitimate to project the covert information into $null\left(\tilde{A}^{\nu}\right)$ instead of $null\left(G^{\nu}\right)$ [7]. The "loss of information" caused by floating point errors could make the evaluation of $null\left(G^{\nu}\right)$ prohibitively unstable for many applications. Specifically, this operation squares the condition number, resulting in the large singular values being increased and the small singular values decreased. This instability is used to the advantage of the designer to increase the security of the covert information.

Assuming the availability of $\tilde{A}^{\nu}$ and $|p^{\nu}\rangle$, the normalized eigenvectors corresponding to the eigenvalues in the *null space* of G^{ν} having value zero (*zero eigenvalues*) is: $|\eta_n^{\nu}\rangle\,; n = 1, ..., N - (M+1)$. The $|\eta_n^{\nu}\rangle$ are hereafter referred to as the basis of $null\left(G^{\nu}\right)$. The unitary decryption $\hat{U}_{dec}^{\nu} : \Re^{N} \rightarrow \Re^{N-(M+1)}$ and encryption operators $\hat{U}_{enc}^{\nu} : \Re^{N-(M+1)} \rightarrow \Re^{N}$ operators for each ν are:

$$
\begin{aligned}
&\hat{U}_{dec}^{\nu} = \sum_{n=1}^{N-M-1} |n\rangle\,\langle\eta_n^{\nu}|, \\
&and, \\
&\hat{U}_{enc}^{\nu} = \hat{U}_{dec}^{\nu\dagger} = \sum_{n=1}^{N-M-1} |\eta_n^{\nu}\rangle\,\langle n|,
\end{aligned}
\tag{8}
$$

respectively. Note that $\hat{U}_{dec}^{\nu} \bullet \hat{U}_{enc}^{\nu} = I$, where I is the identity operator.

Given a code $|q^{\nu}\rangle \in \Re^{N-(M+1)}$ to be encrypted in a host *pdf* having *hierarchy index* ν, the $N - (M+1)$ components are given by $\langle n \mid q^{\nu}\rangle = q_n^{\nu}; n = 1, ..., N - (M+1)$. The *pdf* of the embedded code is:

$$
|p_c^{\nu}\rangle = \hat{U}_{enc}^{\nu}\,|q^{\nu}\rangle = \sum_{n=1}^{N-M-1} |\eta_n^{\nu}\rangle\,\langle n \mid q^{\nu}\rangle. \tag{9}
$$

The total *pdf* comprising the host *pdf* and the *pdf* of the code is:

$$
|\tilde{p}^{\nu}\rangle = |p^{\nu}\rangle + |p_c^{\nu}\rangle\,. \tag{10}
$$

Since $|p_c^{\nu}\rangle \in null\left(\tilde{A}^{\nu}\right)$, $\tilde{A}^{\nu}\,|p_c^{\nu}\rangle = 0$. In the decryption stage, the reconstructed host *pdf*'s: $|p_r^{\nu}\rangle$, are first obtained. The *pdf*'s of the embedded code is recovered from:

$$
|p_{rc}^{\nu}\rangle = \left|\tilde{p}^{\nu}\right\rangle - |p_r^{\nu}\rangle\,. \tag{11}
$$

basis of an ill-conditioned operator (eg. Section 3.1).

The encrypted code is recovered by the operation:

$$|q_r^\nu\rangle = \hat{U}_{dec}^\nu \, |p_{rc}^\nu\rangle = \sum_{n=1}^{N-M-1} |n\rangle \, \langle \eta_n^\nu \mid p_{rc}^\nu \rangle. \tag{12}$$

The above theory does not, by itself, constitute the strategy to encrypt/decrypt code. This is achieved in two manners,i.e, *symmetric* and *asymmetric* cryptographic strategies [11,12]. Before proceeding further, the concept of a key in the encryption of covert information is briefly explained. The distribution of keys is an issue of primary concern in cryptography and allied disciplines. A key may be a program, a number, or a string of numbers that enables the legitimate recipient of the message (decrypter) to access the covert information. In cryptography, a secret, shared, or private key is an encryption/decryption key known only to the entities that exchange secret messages.

In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. Secret key cryptography is also susceptible to a number of malicious attacks, the most common being the *plaintext attack* [11,12]. By definition, a *plaintext attack* is one where the prior messages have intercepted and decrypted in order to decrypt other messages. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a secret key. The RSA protocol [1] is a prominent example of a public key infrastructure (PKI). A PKI often employs a *key ring strategy*. Specifically, one key is kept secret while the others are made public. PKI is the preferred approach on the Internet. The secret key system is sometimes known as *symmetric* cryptography and the public key system as *asymmetric* cryptography.

In this model, an operator $\tilde{G}^\nu$ is formed by perturbing select elements of G^ν by $\delta G_{i,j}^\nu$. In *symmetric* cryptography, only a single element of G^ν is perturbed. The security of the code may be ensured by adopting an *asymmetric* cryptographic strategy. Here, more than one element of G^ν is perturbed. Each $\delta G_{i,j}^\nu > \delta^\nu$, a threshold. The extreme sensitivity to perturbations of G^ν causes the eigenstructure of $\tilde{G}^\nu = G^\nu + \delta G_{i,j}^\nu$ to substantially differ from that of G^ν, This assertion is valid even for infinitesimal perturbations $\delta G_{i,j}^\nu$. To distinguish operations involving the ill-conditioned operators $\tilde{G}^\nu$, the following change of notation is effected in (9)-(12): $|q^\nu\rangle \to |\tilde{q}^\nu\rangle$,$|\eta_n^\nu\rangle \to |\tilde{\eta}_n^\nu\rangle$, $|p_c^\nu\rangle \to |\tilde{p}_c^\nu\rangle$, $|\tilde{p}^\nu\rangle \to \left|\tilde{p}_{pert}^\nu\right\rangle$,$|p_{rc}^\nu\rangle \to |\tilde{p}_{rc}^\nu\rangle$, and, $|q_r^\nu\rangle \to |\tilde{q}_r^\nu\rangle$. The $|\tilde{\eta}_n^\nu\rangle$ are hereafter referred to as the basis of *null* $\left(\tilde{G}^\nu\right)$.

Determination of the threshold is a vital task in defining the cryptographic keys in this model. This is accomplished by the designer (encrypter) who per-

forms a simultaneous encryption/decryption without effecting perturbations to the operator G^{ν}. Specifically, using (2), the host *pdf*'s are inferred by solving an *inverse MaxEnt problem*. The code $|q^{\nu}\rangle$ having dimension $N-(M+1)$ is formed. The designer implements (9)-(12) for each *hierarchy index* ν. The threshold for the cryptographic key/keys is: $\delta^{\nu} = \| |q^{\nu}\rangle - |q_r^{\nu}\rangle \|$.

3 Implementation of the Encryption/Decryption Strategy

The process of encryption occurs after the host *pdf*'s have been inferred from incomplete constraints for *multiple pdf*'s. This procedure is detailed in Section 4. The terminology in cryptography and allied disciplines refers to two communicating parties as Alice and Bob, and, an eavesdropper as Eve. In this study, the author performs the role of both Alice and Bob by implementing the encryption on an IBM RS-6000 workstation cluster and, the decryption on an IBM Thinkpad running $MATLAB^{\circledR}$ v 7.01.

Herein, the implementation of the encryption/decryption strategy by effecting perturbations $\delta G_{i,j}^{\nu}$ to the operator G^{ν} is described. The procedures are to be implemented for each *hierarchy index* ν. This Section presents the implementation of the encryption/decryption strategies in point form, for the sake of clarity and brevity.

3.1 Encryption

(i.) The host *pdf* $|p^{\nu}\rangle$ is inferred from incomplete constraints by solving (2) as an *inverse MaxEnt problem*. (ii.) The constraint operators $\tilde{A}^{\nu}$ and G^{ν} are evaluated formed, for an *a-priori* specified value of the parameter k^{ν}, from (5). The operator $\tilde{G}^{\nu}$ is formed by perturbing one or more elements of G^{ν} by $\delta G_{i,j}^{\nu} > \delta^{\nu}$, the cryptographic key/keys. (iii.) The basis $|\tilde{\eta}_n^{\nu}\rangle\,; n = 1, ..., N-(M+1)$, are evaluated by operating on $\tilde{G}^{\nu}$ with the $MATLAB^{\circledR}$ routine $null\,(\bullet)$ that employs SVD, or with an equivalent routine. (iv.) The code $|\tilde{q}^{\nu}\rangle$ is generated, and, is encoded into the *null space* of $\tilde{G}^{\nu}$ using (9). (v.) The total *pdf* $\left|\tilde{p}_{pert}^{\nu}\right\rangle$ is obtained using (10).

3.2 Transmission

The statistical encryption model provides two separate manners in which information may be transferred from the encrypter to the decrypter, via a *public*

channel. The first mode is to transmit the constraint operators $\tilde{A}^{\nu}$ and the total *pdf*'s $\left|\tilde{p}^{\nu}_{pert}\right\rangle$. An alternate mode is to transmit the LM's obtained on solving the *inverse MaxEnt problem*(Section 3.1), and, the total *pdf*'s $\left|\tilde{p}^{\nu}_{pert}\right\rangle$. Owing to the large dimensions of the constraint operators $\tilde{A}^{\nu}$, the latter transmission strategy is more attractive. The values of parameters k^{ν} for each *hierarchy index*, and, the cryptography key/keys are transmitted through a *secure/covert channel*. The key/keys are labeled in order to identify the elements of the operator G^{ν} that are perturbed. In the case of *asymmetric* cryptography, some of the keys may be declared public, while keeping the remainder private.

3.3 Decryption

(*vi.*) The legitimate receiver recovers the key/keys $\delta G^{\nu}_{i,j}$ and the parameter k^{ν} from the *covert channel*. (*vii.*) The operators $\tilde{A}^{\nu}$, G^{ν} , and, $\tilde{G}^{\nu}$ are constructed. (*viii.*) The host *pdf* may be recovered in two distinct manners, depending upon the transmission strategy employed. Note that both methods to reconstruct the host *pdf* require the total *pdf* $\tilde{p}^{\nu}_{pert}$ to be provided by the encrypter. First, the scaled incomplete constraints, defined in (6), are obtained by solving $\langle i|\, \tilde{A}^{\nu} \left|\tilde{p}^{\nu}_{pert}\right\rangle = \left|\tilde{d}^{\nu}\right\rangle$. Here, i is a basis vector in $\Re^{M+1}$. This procedure is possible because $|\tilde{p}^{\nu}_{c}\rangle \in null\left(\tilde{A}^{\nu}\right)$. Thus, $\tilde{A}^{\nu}\,|\tilde{p}^{\nu}_{c}\rangle = 0$. The host *pdf* are then computed for each *hierarchy index* by solving the *inverse MaxEnt problem*, using the re-scaled set of incomplete constraints. Alternatively, the host *pdf* may be obtained by solving (2) as a *forward MaxEnt problem*, given the values of the LM's λ^{ν}_{i} ; $i = 1, ..., M$ obtained from the *inverse MaxEnt problem* (Section 3.1). Both methods allow the reconstructed host *pdf*'s $|p^{\nu}_{r}\rangle$ to be obtained with a high degree of precision. (*ix.*) The reconstructed code *pdf* $|\tilde{p}^{\nu}_{rc}\rangle$ is recovered using (11). (*x.*) The reconstructed code $|\tilde{q}^{\nu}_{r}\rangle$ is obtained using (12).

It is important to note that the success of the encryption/decryption strategy is critically dependent upon the exact compatibility of software available to the encrypter and decrypter. Of special importance is the compatibility of the routines to calculate the basis $|\tilde{\eta}^{\nu}_{n}\rangle$.

4 Numerical Simulations

This Section provides numerical simulations to analyze the theory and implementation of the statistical encryption/decryption strategy, presented in Section's 2. and 3., respectively. To demonstrate the efficacy of the theory presented in this paper, it is judicious to compare the *pdf* dependent model with

a *pdf* independent model [8]. These are characterized by the constraint operators $\tilde{A}^{\nu}$ (described in (5) and (6)), and, A (described in (4)), respectively. The following numerical studies perform the encryption/decryption strategy for the case of *asymmetric* cryptography. Section 4.1 demonstrates the inference of the host *pdf*'s from incomplete constraints, using an *inverse MaxEnt* procedure.

The comparative analysis between the *pdf* dependent model and the *pdf* independent model is accomplished using two separate metrics, that define the security of the covert information. Host *pdf*'s that deviate further from the equilibrium state often possess a constraint operator $\tilde{A}^{\nu}$ having a higher condition number, as compared with *pdf*'s that are closer to the equilibrium state. Increasing the condition number of the constraint operator $\tilde{A}^{\nu}$ (or, A) represents one way of securing the integrity of the covert information. The condition numbers of the constraint operators are obtained using the $MATLAB^{®}$ routine $cond\,(\bullet)$. This provides a measure of the sensitivity of $null\,(G)$ and $null\,(G^{\nu})$ to perturbations.

In the *pdf* dependent model, the security of the code is enhanced by the increased sensitivity of $null\,(G^{\nu})$ to perturbations of select elements of the operator G^{ν}, resulting in the operator $\tilde{G}^{\nu}$ with *null space* denoted by $null\left(\tilde{G}^{\nu}\right)$. Within the framework of this model, a more relevant metric of the extreme sensitivity of $null\,(G^{\nu})$ to perturbations, brought about by the introduction of the cryptographic keys $\delta G^{\nu}_{i,j}$, is the distortion of the code *pdf* $|p^{\nu}_{c}\rangle$. Here, $|p^{\nu}_{c}\rangle$ is evaluated from (9), using η^{ν}_{n} (the basis of $null\,(G^{\nu})$). The distorted code *pdf* is $|\tilde{p}^{\nu}_{c}\rangle$, which is calculated from (9) using $\tilde{\eta}^{\nu}_{n}$ (the basis of $null\left(\tilde{G}^{\nu}\right)$). Note that the codes $|\tilde{q}^{\nu}\rangle$ and $|q^{\nu}\rangle$ are identical *kets*.

For the *pdf* dependent model, the *RMS error of encryption* between $|\tilde{p}^{\nu}_{c}\rangle$ and $|p^{\nu}_{c}\rangle$ is defined as: $RMS^{\nu}_{enc} = \frac{\|err^{\nu}_{enc}\|}{\sqrt{length(err^{\nu}_{enc})}}$. Here, $\|err^{\nu}_{enc}\| = \|(|\tilde{p}^{\nu}_{c}\rangle - |p^{\nu}_{c}\rangle)\|$, and, $length\,(err^{\nu}_{enc})$ is the dimension of $(|\tilde{p}^{\nu}_{c}\rangle - |p^{\nu}_{c}\rangle)$. Section 4.3 will exemplify the utility of RMS^{ν}_{enc} in resolving a dichotomy. Specifically, it will be demonstrated that a high value of RMS^{ν}_{enc} is the reason for host *pdf*'s possessing constraint operators with lower condition numbers, sometimes providing a greater degree of security to the encoded covert information, than host *pdf*'s possessing constraint operators with higher condition numbers.

Another measure of the security of the covert information, that is operationally advantageous, is the RMS error of the difference between the encrypted code, and, the code reconstructed without the cryptographic keys. For the *pdf* dependent model, the *RMS error of reconstruction* is: $RMS^{\nu}_{recon} = \frac{\|err^{\nu}_{recon}\|}{\sqrt{length(err^{\nu}_{recon})}}$. Here, $\|err^{\nu}_{recon}\| = \|(|\tilde{q}^{\nu}\rangle - |\tilde{q}^{\nu}_{r1}\rangle)\|$, and, $length\,(err^{\nu}_{recon})$ is the dimension of $(|\tilde{q}^{\nu}\rangle - |\tilde{q}^{\nu}_{r1}\rangle)$.

The rationale for evaluating the RMS^{ν}_{recon} is to obtain a measure of the error of reconstruction by an *unauthorized eavesdropper (Eve)*, who does not possess the correct cryptographic keys $\delta G^{\nu}_{i,j}$. Eve is, however, assumed to be in possession of the reconstructed code *pdf* $|\tilde{p}^{\nu}_{rc}\rangle$. Such an attack may be simulated by choosing the wrong set of keys, and, incorrectly constructing the perturbed operators $\tilde{G}^{\nu}$ and $\tilde{G}$. Alternatively, an analogous scenario may be simulated by assuming that the reconstruction is performed without keys (*sans* keys). In this case, the reconstructed code without keys is: $|\tilde{q}^{\nu}_{r1}\rangle = \sum_{n=1}^{N-M-1} |n\rangle \langle \eta^{\nu}_n \mid \tilde{p}^{\nu}_{rc}\rangle$. Here, η^{ν}_n is the basis of $null\,(G^{\nu})$. Section 4.2 presents the comparative analysis using the performance metrics described above. Analysis of the results is provided in Section 4.3.

4.1 Inference of the host pdf's

Host *pdf* column vectors (*kets*) corresponding to *hierarchy indices* $\nu = 1$ and $\nu = 2$, each of dimension 401, are independently inferred in the event space $[-1, 1]$. The incomplete constraints are the first four moments of the random variable $x_n; n = 1, ..., N$. From (2), one obtains:

$$d^{\nu}_i = \frac{\sum\limits_{n=1}^{N=401} x^i_n e^{-\lambda^{\nu}_1 x_n - \lambda^{\nu}_2 x^2_n - \lambda^{\nu}_3 x^3_n - \lambda^{\nu}_4 x^4_n}}{\sum\limits_{n=1}^{N=401} e^{-\lambda^{\nu}_1 x_n - \lambda^{\nu}_2 x^2_n - \lambda^{\nu}_3 x^3_n - \lambda^{\nu}_4 x^4_n}}; i = 1, ..., M = 4 \tag{13}$$

Here, (13) is solved as an *inverse MaxEnt problem* for two different sets of incomplete constraints (corresponding to each *hierarchy index*), provided as input values. These are $d^{\nu=1}_1 = -0.0224, d^{\nu=1}_2 = 0.1048, d^{\nu=1}_3 = -0.0124, d^{\nu=1}_4 = 0.0284$, and, $d^{\nu=2}_1 = 0.1, d^{\nu=2}_2 = 0.3, d^{\nu=2}_3 = 0.1, d^{\nu=2}_4 = 0.15$, respectively. Note that the values of $d^{\nu=1}_i$, are taken to be the same as those in [8].

Each *hierarchy index* yields $M + 1$ constraint equations, that are solved using a Newton-Raphson procedure. Note that the $(M + 1)^{st}$ constraint equation follows from the *pdf* normalization condition. The values of the LM's are found to be $\lambda^{\nu=1}_1 = -0.30435, \lambda^{\nu=1}_2 = 2.99664, \lambda^{\nu=1}_3 = 4.85637, d^{\nu=1}_4 = 3.81359$, and, $\lambda^{\nu=2}_1 = 1.74906, \lambda^{\nu=2}_2 = -5.09475, \lambda^{\nu=2}_3 = -4.8568, \lambda^{\nu=2}_4 = 8.48337$, respectively.

In this example, each constraint operator $\tilde{A}^{\nu}$ is of dimension 5×401 , and, the number of basis $\tilde{\eta}^{\nu=1,2}_n$ is 396, for each *hierarchy index*. Figure 1 depicts the two host *pdf*'s. The case with *hierarchy index* $\nu = 1$ is the single peaked *pdf*, while the case with *hierarchy index* $\nu = 2$ is the double peaked *pdf*.

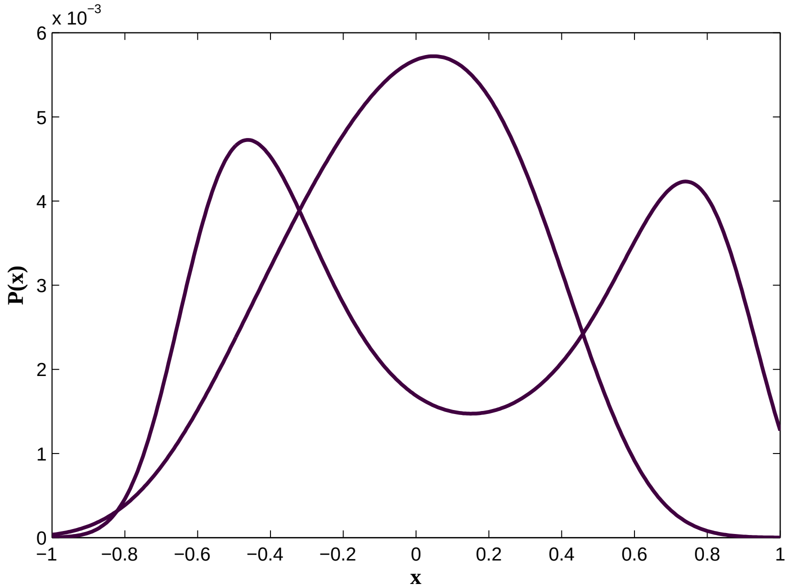

Fig. 1. Host *pdf*'s inferred from incomplete constraints for $\nu = 1$ and $\nu = 2$

4.2 Comparative analysis

The $MATLAB^{®}$ random number generator $rand\,(\bullet)$ is evoked to generate code in $[0, 1]$. In order to establish a degree of uniformity in the comparisons, two identical *kets* of the code, each having dimension $N-(M+1)$ i.e. 396, are created for projection into the *null spaces* of the perturbed operators $\tilde{G}^{\nu}$ and $\tilde{G}$, respectively. This "emulates" the *selective* projection of a code comprising of a single *ket* of dimension 792, into $null\left(\tilde{G}^{\nu=1,2}\right)$ and $null\left(\tilde{G}\right)$, for each *hierarchy index*.

A further measure of uniformity in the comparative analysis is sought by specifying the perturbations to both G and G^{ν} as $\delta G_{1,3} = \delta\tilde{G}^{\nu=1,2}_{1,3} = 3.0e-013$ (first row, third column) and $\delta G_{2,7} = \delta\tilde{G}^{\nu=1,2}_{2,7} = 7.0e-013$ (second row, seventh column), respectively. All numerical examples in this paper have a threshold for perturbations $\delta^{\nu} \sim 4.4e-014$.

Simulations for the case of the *pdf* independent model are described in Section 4.2.1. Two distinct case studies for the *pdf* dependent model are described in Sections 4.2.2 and 4.2.3, respectively. The results are presented in Table 1 through Table 3. Therein, sample values of the original code, the code reconstructed *with* the keys, and, the code reconstructed *without* the keys are presented. These comprise the $1^{st}, 75^{th}, 177^{th}, 296^{th}, and, 395^{th}$ elements of the respective arrays (*kets*). As is evident from the numerical simulations, the reconstructed code *with* the keys is exactly similar to the original code. The corresponding RMS^{ν}_{recon} is zero. On the other hand, the code reconstructed without the keys bears no resemblance to the original code.

Table 1
Select code values for the *pdf* independent model. $|q^{\nu}\rangle$ - the original code, $|q_r^{\nu}\rangle$ - the code reconstructed *with* the keys, and, $|q_{r1}^{\nu}\rangle$ - the code reconstructed *without* the keys.

$\left\|q^{\nu=1,2}\right\rangle$	$\left\|q_r^{\nu=1,2}\right\rangle$	$\left\|q_{r1}^{\nu=1,2}\right\rangle$
0.23813682639005	0.23813682639005	-0.09239755885631
0.69913526160795	0.69913526160795	0.20008072567388
0.27379424177629	0.27379424177629	-0.16469110441464
0.17686701421432	0.17686701421432	0.92507582836680
0.20288628732009	0.20288628732009	-0.51825561367528

Table 2
Select code values for the *pdf* dependent model-case study 1. $|\tilde{q}^{\nu}\rangle$ - the original code, $|\tilde{q}_r^{\nu}\rangle$ - the code reconstructed *with* the keys, and, $|\tilde{q}_{r1}^{\nu}\rangle$ - the code reconstructed *without* the keys.

$\left\|\tilde{q}^{\nu=1,2}\right\rangle$	$\left\|\tilde{q}_r^{\nu=1,2}\right\rangle$	$\left\|\tilde{q}_{r1}^{\nu=1}\right\rangle$	$\left\|\tilde{q}_{r1}^{\nu=2}\right\rangle$
0.23813682639005	0.23813682639005	-0.08237185729405	0.40428740297403
0.69913526160795	0.69913526160795	-0.01133471359936	0.30190786147110
0.27379424177629	0.27379424177629	-0.33080751552396	-0.29261640748833
0.17686701421432	0.17686701421432	-1.18947579992697	0.53834101226185
0.20288628732009	0.20288628732009	0.54528163427934	-0.10688384159491

4.2.1 Pdf independent model

Here, $cond\,(A) = 18.80458$, $RMS_{enc}^{\nu=1,2} = 0.76998$, and, $RMS_{recon}^{\nu=1,2} = 0.77483$. The values of the encrypted and reconstructed codes are independent of the *hierarchy index*. These results are consistent with expectations since the nature of the host *pdf* is not reflected in the constraint operator A. Select code values are presented in Table 1.

4.2.2 Pdf dependent model : case study 1

The parameters are $k^{\nu=1} = 0.065$, and, $k^{\nu=2} = 0.09$. Here, $cond\left(\tilde{A}^{\nu=1}\right) = 19.87136$, $RMS_{enc}^{\nu=1} = 0.79533$, and, $RMS_{recon}^{\nu=1} = 0.80034$. Further, $cond\left(\tilde{A}^{\nu=2}\right) = 20.42975$, $RMS_{enc}^{\nu=2} = 0.82570$, and, $RMS_{recon}^{\nu=2} = 0.83090$. This case represents a noticeable increase in the level of security of the code, and flexibility of the theory, as compared with the *pdf* independent model. Select code values are presented in Table 2.

Table 3
Select code values for the *pdf* dependent model-case study 2. $|\tilde{q}^{\nu}\rangle$ - the original code,$|\tilde{q}_r^{\nu}\rangle$ - the code reconstructed *with* the keys, and, $|\tilde{q}_{r1}^{\nu}\rangle$ - the code reconstructed *without* the keys.

$\left\|\tilde{q}^{\nu=1,2}\right\rangle$	$\left\|\tilde{q}_r^{\nu=1,2}\right\rangle$	$\left\|\tilde{q}_{r1}^{\nu=1}\right\rangle$	$\left\|\tilde{q}_{r1}^{\nu=2}\right\rangle$
0.23813682639005	0.23813682639005	0.41205157405440	-1.47600706971518
0.69913526160795	0.69913526160795	0.96359310993344	-0.12406066610739
0.27379424177629	0.27379424177629	-0.03625400789579	0.71289692833557
0.17686701421432	0.17686701421432	-0.94767053576282	-0.37638356088402
0.20288628732009	0.20288628732009	-0.87540038881240	0.57110616844674

4.2.3 Pdf dependent model :case study 2 - a study in contrast

The parameters are $k^{\nu=1} = -0.03$, and, $k^{\nu=2} = -0.5$. Here, $cond\left(\tilde{A}^{\nu=1}\right) = 18.31597$, $RMS_{enc}^{\nu=1} = 0.81620$ and, $RMS_{recon}^{\nu=1} = 0.82134$. Further, $cond\left(\tilde{A}^{\nu=2}\right) = 11.97782$, $RMS_{enc}^{\nu=2} = 0.84434$, and, $RMS_{recon}^{\nu=2} = 0.84965$. This case represents a noticeable increase in the level of security of the code in terms of $RMS_{recon}^{\nu=1,2}$, the RMS error of reconstruction, as compared with the results in Sections 4.2.1 and 4.2.2, respectively. Select code values are presented in Table 3.

4.3 Analysis of results

The case presented in Section 4.2.2 follows expectations. Specifically, the constraint operators $\tilde{A}^{\nu=1,2}$ possess larger condition numbers than the constraint operator A of the *pdf* independent model, presented in Section 4.2.1. Further, the $RMS_{enc}^{\nu=1,2}$ and $RMS_{recon}^{\nu=1,2}$ in the *pdf* dependent model are greater those for the *pdf* independent model. This implies that the *pdf* dependent model provides greater security to the covert information, than the *pdf* independent model. The case presented in Section 4.2.3 represents an interesting scenario, which poses a dichotomy of sorts.

Conventional logic would expect an increase in the condition numbers of $\tilde{A}^{\nu=1,2}$ to coincide with an increase in the sensitivity of $null\left(G^{\nu=1,2}\right)$, and thus, an increase in the values of $RMS_{recon}^{\nu=1,2}$. Section 4.2.3 conclusively demonstrates the fact that the condition number of $\tilde{A}^{\nu}$ and the RMS_{recon}^{ν} do not necessarily increase simultaneously. Specifically, the case presented in Section 4.2.3 demonstrates a significant *decrease* in the condition numbers of $\tilde{A}^{\nu=1,2}$, that is accompanied by a significant *increase* in $RMS_{recon}^{\nu=1,2}$.

This dichotomy may be explained by the fact that an *increase* in the value

of $RMS_{recon}^{\nu=1,2}$ is always accompanied by a corresponding *increase* in the RMS error of encryption: $RMS_{enc}^{\nu=1,2}$. This trend is evident in each of the case studies presented in this paper, and, has been consistently observed in numerous simulation exercises. As indicated in the introduction of Section 4, the RMS error of encryption (RMS_{enc}^{ν}) represents a more relevant metric to assess the sensitivity of $null\,(G^{\nu})$ to perturbations $\delta G_{i,j}^{\nu}$, as compared to the condition number of A^{ν}, within the framework of this statistical encryption/decryption model.

This Section is concluded by providing a glimpse of the effects of the instability of the eigenstructures of the ill-conditioned operators. Figure 2 depicts the error of encryption: $|\tilde{p}_c^{\nu}\rangle$ - $|p^{\nu}\rangle$ for the case study presented in Section 4.2.3, corresponding to $k^{\nu=2} = -0.5$ The highly oscillatory ("chaotic") profile in Figure 2 is indicative of the extreme sensitivity of $null\,(G^{\nu})$ to perturbations $\delta G_{i,j}^{\nu}$ applied to G^{ν}.

It may be noted that the code $|\tilde{q}^{\nu}\rangle$, projected into each host *pdf*, comprises of a *ket* of dimension 396 created by a random number generator. While one might expect the randomness inherent in $|\tilde{q}^{\nu}\rangle$ to be factored into the error of encryption, further investigation concerning the oscillatory behavior is required. The *ket* $|\tilde{q}^{\nu}\rangle$ is subjected to a sorting operation, by employing the $MATLAB^{\circledR}$ routine $sort\,(\bullet)$. This results in a *ket* $|\tilde{q}^{\nu}\rangle$ of dimension 396, containing progressively increasing values defined in $[0, 1]$. The resulting error of encryption using the sorted code is depicted in Figure 3.

As is observed, the error of encryption still displays a highly pronounced oscillatory behavior, despite the randomness in the code being mitigated. Akin to the case depicted in Figure 2, this oscillatory behavior is reflective of the instability induced in $null\,(G^{\nu})$ by perturbing 2 elements of G^{ν} (having dimension 401×401) by $3.0e-013$ and $7.0e-013$, respectively. Figure 4 depicts the total *pdf* defined by (10), corresponding to the case study presented in Section 4.2.3 for $\nu = 2$. As is expected, the total *pdf* exhibits a highly oscillatory ("chaotic") behavior. This is in stark contrast to the smooth curves of the host *pdf*'s depicted in Figure 1.

5 Summary and Conclusions

A novel strategy to project covert information into a hierarchy of statistical hosts has been presented. This has been accomplished within the ambit of the MaxEnt principle. The encryption/decryption strategy relates the projection of the covert information to the host *pdf*'s. This feature permits the statistical encryption/decryption strategy to possess immense qualitative flexibility, and, provide enhanced security to the covert information, as compared to a *pdf*

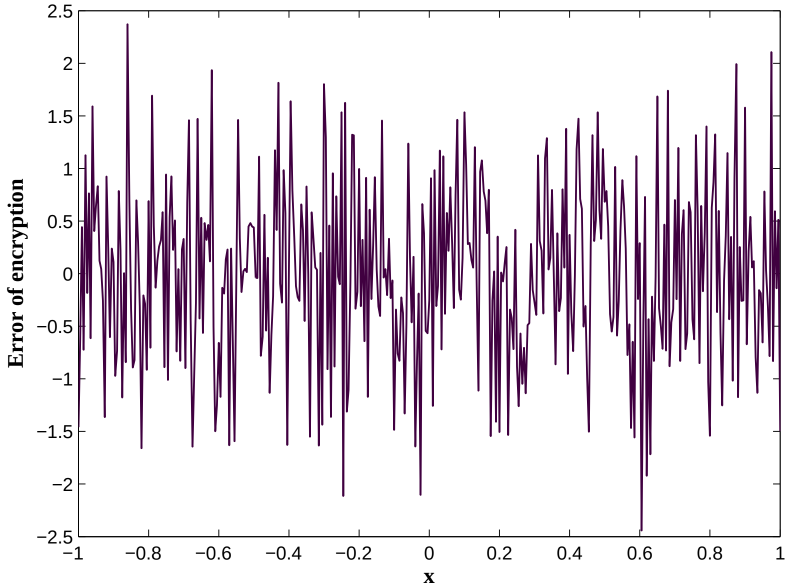

Fig. 2. Plot of the error of encryption: $|\tilde{p}_c^\nu\rangle$- $|p_c^\nu\rangle$.

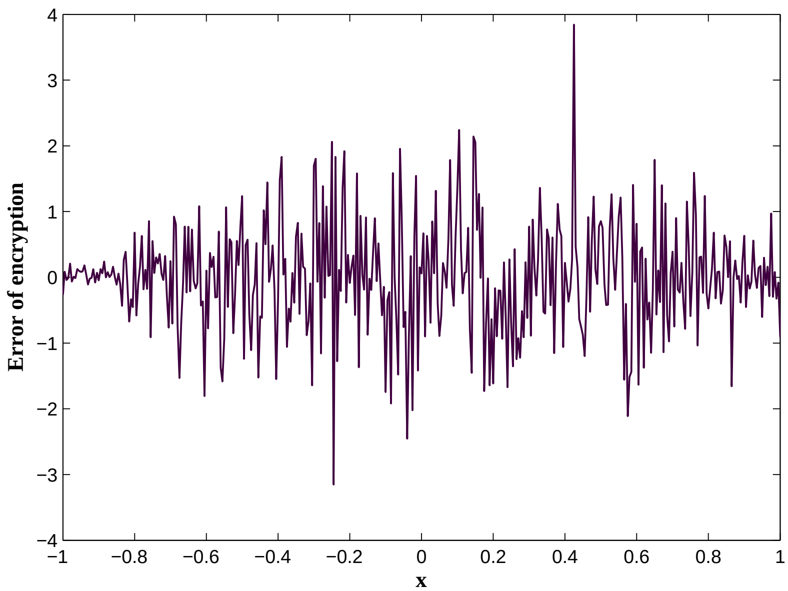

Fig. 3. Plot of the error of encryption: $|\tilde{p}_c^\nu\rangle$- $|p_c^\nu\rangle$ with sorted code.

independent model [8].

The *pdf* dependent model, presented herein, sometimes demonstrates an increased RMS error of reconstruction for decreased values of the condition number of the constraint operator A^ν. This seemingly counter-intuitive result is adequately explained with the aid of the RMS error of encryption. The RMS error of encryption is demonstrated to be a viable and relevant metric to assess the sensitivity of $null\,(G^\nu)$ to perturbations $\delta G^\nu_{i,j}$.

The statistical encryption/decryption strategy is platform independent, and

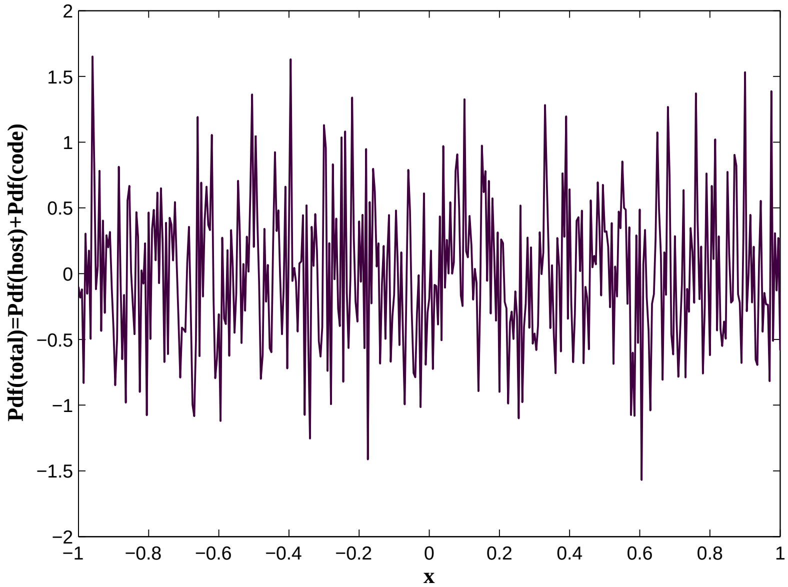

Fig. 4. "Chaotic" nature of the total *pdf* = host *pdf* + code *pdf*

the process of recovery of the covert information is accomplished with a very high degree of precision. The small amounts of data being transmitted through the covert channel as a consequence of the transmission of the cryptographic keys $\delta G^{\nu}_{i,j}$ and the *hierarchy indices* k^{ν}'s (see Section 3.2), augers well for a coupling between the statistical encryption/decryption model, and a quantum key distribution protocol [13, 14].

A study extending the present work, by describing the statistical encryption/decryption strategy within the framework of a Fisher-Schrödinger model, has been recently completed. Herein, the Fisher information has been employed as the measure of uncertainty. The host *pdf*'s satisfy a time independent Schrödinger-like equation (TISLE) with an empirical *pseudo-potential*, that approximates a time independent Schrödinger equation (TISE) physical potential [7, 15] . The TISLE inherits the *energy states* of the TISE, within an information theoretic context. The encryption of covert information is tantamount to projection of the code into different *energy states* of the TISLE. The *hierarchy indices* in the present paper are replaced by the TISLE *energy states*.

The Fisher-Schrödinger model provides a quantum mechanical connotation to the statistical encryption/decryption strategy. Coupling the Fisher-Schrödinger model with a quantum key distribution protocol holds forth the prospect of achieving a self-consistent *hybrid* statistical/quantum mechanical cryptosystem. This work will be shortly presented for publication.

Ongoing work is directed towards a two-pronged objective. First, the projection of the covert information into $null\,(G^{\nu})$ has been provided with an information theoretic basis. Next, models to extend the work presented in

this paper to the case of steganography and information hiding have been developed.

By definition, steganography involves hiding data inside other (host) data. In steganography, the covert information is concealed in a manner such that no one apart from the intended recipient knows of the existence of the message. This is in contrast to cryptography, where the existence of the message is obvious, but the meaning is obscured. The extension of the statistical encryption/decryption model presented in this paper to steganography involves encrypting image data into a *cover image*. In this case, the average pixel intensities of the *cover image* constitute the incomplete constraints. These results will be presented in future publications.

Acknowledgements

This work was supported by *MSR contract CSM-DI & S-QIT-101107-2005*. Gratitude is expressed to A. Plastino, L. Rebollo-Neira, and B. R. Frieden for helpful discussions.

References

[1] R. L. Rivest, A. Shamir, L. Adelman, "On Digital Signatures and Public Key Cryptosystems," *MIT Laboratory for Computer Science Technical Memorandum*, **82**, Massachusetts Institute of Technology (1977).

[2] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms", *IEEE Transactions on Information Theory* **31** (1985) 469-472.

[3] V. Miller, "Use of Elliptic Curves in Cryptography", in H. C. Williams (Ed.), *Advances in Cryptology – CRYPTO '85*, Lecture Notes in Computer Science, Springer-Verlag, New York 417-426, 1986.

[4] E. T. Jaynes, *Probability Theory, the Logic of Science*, Cambridge University Press, Cambridge, 2003.

[5] S. Katzenbeisser and F. A. Petitcolas, *Information Hiding: Techniques for Steganography and Digital Watermarking*, Artech House, Norwood MA, 2000.

[6] P. Moulin and J. A. O'Sullivan, "Information-Theoretic Analysis of Information Hiding", *IEEE Transactions on Information Theory*, **49**(3) (2003) 563-593.

[7] R. C. Venkatesan, "Encryption of Covert Information through a Fisher Game", in *Exploratory Data Analysis Using Fisher Information*, B. R. Frieden and R. A. Gatenby (Eds.), Springer-Verlag, London, 2006 (in press).

[8] L. Rebollo-Neira and A. Plastino, "Statistical Distribution, Host for Encrypted Information" *Physica A* ,**359** (2006) 213-221.

[9] P. A. M. Dirac, *Principles of Quantum Mechanics (The International Series of Monographs on Physics)*, Oxford University Press, Oxford, 1982.

[10] G. H. Golub and C. F. van Loan, *Matrix Computations*, 3rd edn, Johns Hopkins University Press, Baltimore, 1995.

[11] J. A. Buchmann, *Introduction to Cryptography*, Springer, London, 2004.

[12] B. Schneier, *Applied Cryptography*, 2nd edn. John Wiley & Sons, New York, 1996.

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[14] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", in *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing*, Bangalore, India, IEEE Press, New York, 175-179, 1984.

[15] B. R. Frieden, *Science from Fisher Information: A Unification*, Cambridge University Press, Cambridge, 2004.